

**DEPARTMENT OF STATE**  
**FISCAL YEAR 2008**  
**PRIVACY IMPACT ASSESSMENT**  
**DEPARTMENT OF STATE (DoS)**  
**CLEARANCE SYSTEM**

**Conducted by:**  
**Bureau of Administration**  
**Information Sharing Services**  
**Office of Information Programs and Services**  
**Privacy (PRV)**  
**Email: [PIA@state.gov](mailto:PIA@state.gov)**

**A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION**

- 1) Does this system collect, maintain or disseminate personally identifiable information about individual members of the public\*\*?

YES X NO     

The Clearance System is a major application which does not collect any information. However, the System serves as a platform for various major applications used within Diplomatic Security that contain PII. The specific PII pertaining to the major applications is detailed in their systems PIAs.

**\*\* “Personally identifiable information from/about individual members of the public” means personally identifiable information from/about “any person not acting in his/her official capacity as a federal government employee/contractor”.**

If answer is yes, please complete the survey in its entirety.

If answer is no, please complete the certification page and submit the completed PIA to both of the following e-mail address: pia@state.gov

- 2) Does a Privacy Act system of records already exist?

YES X NO     

If yes, please provide the following:

System Name Diplomatic Security Records Number STATE-36

“A new System of Records Notice (SORN) is **not** necessary.”

If no, a Privacy system of records description will need to be created for this data.

- 3) What is the purpose of the system/application?

The Department of State Clearance System is a major application that supports Diplomatic Security mission requirements in assigning, tracking, and completing investigative leads and subsequently this information assists with the determination of granting personnel security clearances for DoS employees via DS/SI/PSS and contractor staff via DS/IS/IND.

- 4) What legal authority authorizes the purchase or development of this system/application?

The legal authorities as documented in STATE-36, Diplomatic Security Records.

## **C. DATA IN THE SYSTEM**

### **1) What categories of individuals are covered in the system?**

The categories of individuals that are covered by the system are documented in STATE-36, Diplomatic Security Records.

### **2) What are the sources of the information in the system?**

#### **a. Who/what is the source of the information?**

The source of the information is the individual or law enforcement agency(ies).

#### **b. What type of information is collected from the source of the information?**

The Department of State (DoS) Clearance System is a major application that supports Diplomatic Security mission requirements in assigning, tracking, and completing investigation leads and subsequently granting personnel security clearances for DoS employees via DS/SI/PSS and contractor staff via DS/IS/IND. DoS Clearance System captures data/information relevant to an investigated case, for example;

- Name;
- Date of birth;
- Address;
- Telephone number;
- Financial statement; and
- Other personally identifiable information (PII) specific to the Department employee or contractor under investigation.

### **3) Accuracy, Timeliness, and Reliability**

#### **a. How will data collected from sources other than DOS records be verified for accuracy?**

The agency or source providing the information is responsible for verifying accuracy. In this case, the Bureau of Diplomatic Security (DS) is responsible for verifying accuracy.

#### **b. How will data be checked for completeness?**

Completeness of data will be checked through investigations and/or through personal interviews of the source of the information.

#### **c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).**

Investigations and/or through personal interviews will confirm whether data is current.

#### **D. INTENDED USE OF THE DATA**

**1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?**

The Department of State Clearance System is a major application that supports Diplomatic Security mission requirements in assigning, tracking, and completing investigation leads and subsequently granting personnel security clearances for DoS employees via DS/SI/PSS and contractor staff via DS/IS/IND. DoS Clearance System captures data/information relevant to an investigated case, for example;

- Name;
- Date of birth;
- Address;
- Telephone number;
- Financial statement; and
- Other personally identifiable information (PII) specific to the Department employee or contractor under investigation.

**2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?**

Yes. An aggregation of data from other federal agencies will be gathered to provide a complete picture of the Department Employee or Contractor under consideration for a security clearance.

**3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?**

Yes. The information will assist in determining whether to allow a potential/current DS employee or contractor to remain as a representative of the Bureau of Diplomatic Security (from an employment perspective).

**4) Will the new data be placed in the individual's record?**

Yes. The information will be added to the biographical information maintained on the individual.

**5) How will the new data be verified for relevance and accuracy?**

Verification will be made through investigations and/or personal interviews.

**6) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

The identification of data pertaining to an individual is retrieved by the use of a personal identifying number (PIN) assigned by the system.

**7) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

Various reports are provided by the system for statistical, law enforcement, and management purposes. These reports are used by Department of State personnel and are “Sensitive but Unclassified” and not for release outside of the State Department without prior approval.

**E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS**

- 1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The System is operated at one site-- State Annex-20 (SA-20).

- 2) What are the retention periods of data in this system?**

The retention period for data is consistent with established Department of State policies and guidelines as documented in the Department's Disposition Schedule of Diplomatic Security Records, Chapter 11.

- 3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

The retention period of data is consistent with established Department of State policies and guidelines as documented in the Department's Disposition Schedule of Diplomatic Security Records, Chapter 11.

- 4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No.

- 5) How does the use of this technology affect public/employee privacy and does it restrict access to the system?**

No additional or new effect to public/employee privacy. Access restrictions are in place.

- 6) If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

No, the system does not provide the capability to identify, locate, and monitor individuals.

- 7) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

N/A. The system/application will not be modified to the point at which a new system of records notice (SORN) will be required. The current system of records is sufficient.

- 8) **Are there forms associated with the system? YES \_\_\_\_ NO \_\_X\_\_**  
**If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?**

**F. ACCESS TO DATA**

- 1) **Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?**  
Access to the data in the system is on a “need-to-know” basis and/or under routine use criteria as explained in STATE-36.
- 2) **What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?**  
A criterion for gaining access to the system is on a “need-to-know” basis. Criteria, procedures, controls, and responsibilities regarding access are all documented.
- 3) **Will users have access to all data on the system or will the user’s access be restricted? Explain.**  
Access will be restricted on a need to a “need to know basis” specific to work related responsibilities.
- 4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)**  
The system provides a means of limiting access to areas within the application based on user ID, password, and a “need-to-know.” Moreover, the Bureau of Diplomatic Security employees and contractors must follow the System Behavior Rules established by the Department.
- 5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? Yes**  
  
**If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Yes**

**Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**  
Yes

**6) Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface? No.**

**7) Will other agencies share data or have access to the data in this system (Federal, State, Local, and Other)? If so, how will the data be used by the other agency?**

Other agencies will not have direct access to the data but the data may be shared with an agency upon request if that agency is listed as a routine user in STATE-36. The use of the data by the other agency will be restricted to the same purpose for which the data was originally collected.

**8) Who is responsible for assuring proper use of the SHARED data?**

The agency receiving the information is responsible for adhering to lawful restrictions.